IS BIGGER BETTER?

HOW SMALL & MIDSIZED ORGANIZATIONS ARE BETTER AT CLOSING THE IoT SECURITY GAP THAN LARGER COMPETITORS

A 2017 IoET SUPPLEMENTAL REPORT

PWNIE EXPRESS

@PwnieExpress

TABLE OF CONTENTS

TABLE OF GRAPHS

INTRODUCTION

IoT technology is creating dynamic new possibilities for consumers, businesses, and governments. However, connecting all aspects of an organization's business is both a blessing and a curse. IoT creates a vast attack surface that is easy for threat actors to penetrate and manipulate. The more connected you get, the more vulnerable you become. Unfortunately, you can't secure IoT with traditional security measures.

We call this opening in an organization's defenses created by the arrival of IoT devices "the IoT security gap." IT security professionals are beginning to realize you won't close this gap with the existing tools in your digital arsenal. You need IoT-specific security measures to catch threat actors attempting to gain access to your systems via connected devices like medical devices, manufacturing sensors, webcams, printers and even the new coffee maker in the kitchenette.

Left unaddressed, the IoT security gap puts newly connected parts of businesses at significant risk. Addressed, enterprises can differentiate from their competition and optimize business operations with the successful adoption of IoT.

Attempting to close the IoT security gap with traditional security tools, is similar to deciding to take off in the fog with no instruments and precious cargo. Sure, you are going faster than your competition who is driving, but good luck detecting that mountain in front of you.

The Pwnie Express IoT security platform identifies all devices, assesses threats, and prevents IoT based attacks. To learn more, go to pwnieexpress.com.

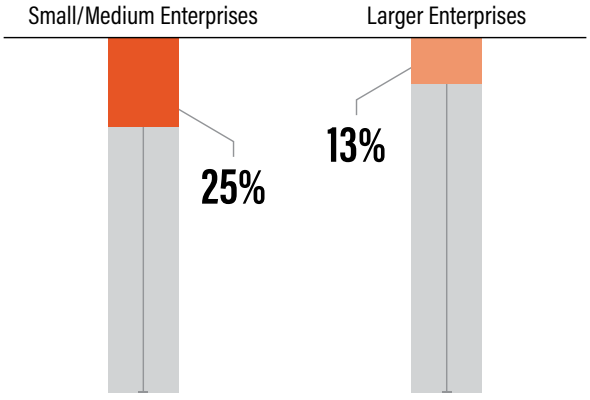
2017 INTERNET OF EVIL THINGS—A REVIEW OF KEY FINDINGS

IoT THREATS ACROSS THE BOARD

IoT poses significant security issues whether you are a organization of 50 or 50 thousand. The 2017 IoET report revealed that 39 percent of organizations are unprepared to handle connected device threats, only 40 percent have the capability to track on-network IoT devices, and just eight percent are able to track off-network IoT devices.

Research by Gartner, the world's leading information technology research and advisory company, showed security was cited as the top barrier to IoT success by 35 percent of respondents.[1] In our research, 25 percent of SMOs said budget limitations were the largest barrier to making their companies more secure. Thirteen percent of the largest organizations said budgets were their biggest problems.

GRAPH 01 **WHAT IS THE LARGEST BARRIER TO MAKING YOUR COMPANY MORE SECURE?**



But events could be forcing organizations to re-prioritize. Last fall, the malware known as Mirai spread through hundreds of thousands of IoT connected devices, turning infected webcams, printers, and routers into a large and powerful zombie botnet army. The attack even had an effect on more knowledgeable IT security professionals. 84 percent of those we surveyed admitted that Mirai changed their perception about threats from IoT devices.

Yet, more than 65 percent say they either haven't checked or don't know how to check their connected devices for Mirai. With Mirai and its inspired offshoots in the wild, determined attackers see the potential to use vulnerable connected devices for nefarious large-scale purposes and to target and compromise specific networks and companies.

The professionals need new tools to find the threats now exploiting IoT. IoT security solutions must break from traditional thinking and continuously identify and assess the risks associated with all connected devices in order to prevent threats from impacting critical business operations.

To see more about the research on ransomware, man-in-the-middle attacks, please go to the Pwnie Express website and download the full report.

WHAT WE'VE SEEN SINCE THE IoET REPORT

While most IoT is a whole new area of technology, we've also seen how threat actors can target older systems. In the biggest ransomware attack in history, known as "WannaCry", 98 percent of the attacks hit

devices using Windows 7 and older.[2] The attacks also demonstrated how hospitals (like Britain's National Health Service or NHS), car factories (Honda, Nissan, and Renault) and phone companies (Spain's Telefonica) have now connected these older systems to the rest of their business.

The Mirai, WannaCry, and GoldenEye attacks have exposed key vulnerabilities to threat actors around the world. This problem will not go away. Organizations must learn from the mistakes experienced at the beginning of the 21st century when businesses first realized the threats from attackers targeting hardwired devices. As we did a deeper dive into our IoET survey, we found that some organizations have taken steps to protect themselves from these new threat vectors.

WHO IS BETTER PREPARED FOR THE NEXT ATTACK? SMALL AND MIDSIZED ORGANIZATIONS OR LARGE ORGANIZATIONS?

When it comes to cybersecurity, it is usually assumed that bigger organizations with larger IT budgets have better defenses and are more prepared to fight cyber intrusions. After all, larger organizations have more trading partners and more customers—for the most part—and would appear to stand to lose the most from a cyber attack.

We thought that when we took the data from our 2017 Internet of Evil Things research and broke it down by small and midsized organizations (SMOs) versus large organizations, we'd see the large organizations were better armed to manage a threat. But, conventional wisdom isn't always true.

When we reviewed the answers from the 950 IT security professionals who took our survey, we saw that SMOs are more aware of the IoT devices on their network and more prepared to handle connected device threats.

A cyber attack on a large organization always hurts, but can be weathered. An attack on a small business with more limited resources can be deadly.

Perhaps, that is why we are increasingly finding that SMOs are taking the lead in protecting themselves against the ever-increasing risks associated with the Internet of Things (IoT).

THE SMALL ORGANIZATION STORY

Small organizations (less than 1,000 employees) can be quickly overwhelmed with burdensome unbudgeted expenses for cyber insurance, legal aid, and increased cybersecurity measures to protect against ransomware attacks. Sometimes, the fallout after the payment deadline has passed can be worse than the attack itself. Several research reports have shown small/midsized organizations face horrendous burdens trying to fend off an onslaught by threat actors. Consider just some of the numbers:

- The National Cyber Security Alliance found that 60 percent of small/medium organizations that face a cyber attack declare bankruptcy in 6 months.[3]
- The average cost that a small organization incurs when dealing with a cyberattack is $690,000.[4]
- 50 percent of small-midsized businesses have been breached in the past 12 months.[5]
- Just 13 percent of small businesses rated their company's preparedness to deal with ransomware attacks as "high."[6]

While many people have rushed to get the newest and coolest gadgets and gizmos on the market, others realize many connected webcams, printers, and coffeemakers need to be monitored closely. Perhaps smaller organizations, burned by past experiences, are more determined to get out in front of the threat from a new generation of connected devices? That might explain why in our survey, small and midsized organizations were doing much more to check connected devices than their larger counterparts.

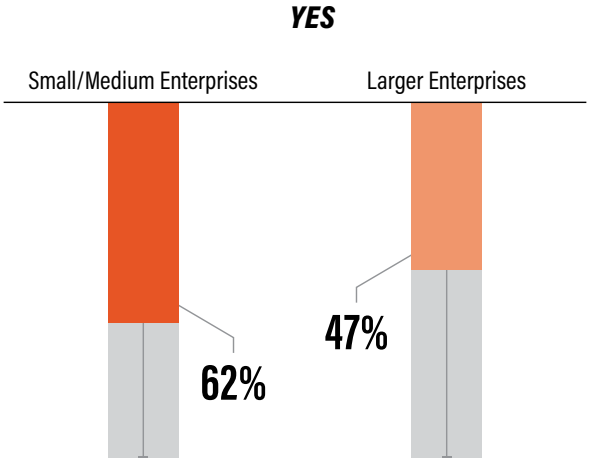
WHAT THE SMALL ORGANIZATIONS ARE DOING RIGHT

Our IoET research showed that many of those working for smaller and midsized organizations (we surveyed 610) are better than larger organizations at implementing and executing measures to protect their employers from threats coming into their offices.

In fact, we found several examples of small-to-midsized organizations performing better than their larger counterparts when it comes to cyberhygeine:

→ 62 percent of SMOs know how many devices are connected to their networks as compared to 47 percent of large organizations.

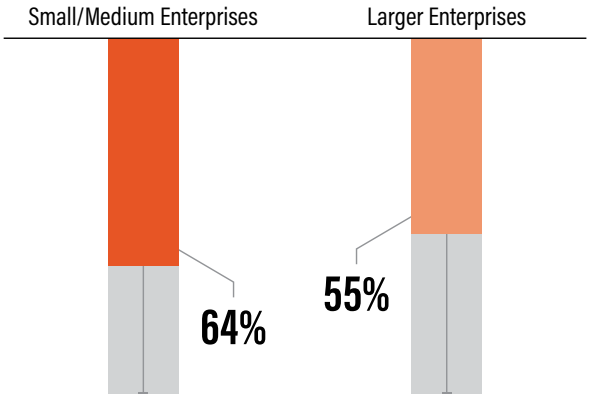
GRAPH 02 **DO YOU KNOW HOW MANY DEVICES ARE CONNECTED TO YOUR NETWORK?**



→ 64 percent of SMOs have checked wireless devices in the workplace for malicious infection in the last month compared to 55 percent of larger organizations.

GRAPH 03 **WHEN WAS THE LAST TIME YOU CHECKED YOUR WIRELESS DEVICES FOR MALICIOUS INFECTIONS?**

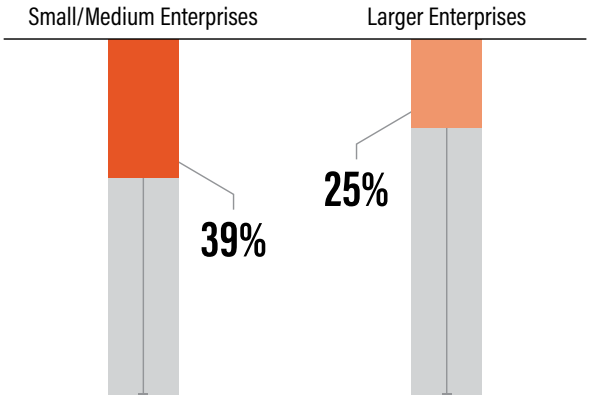
IN THE LAST MONTH



→ SMOs are much more aware of how many connected devices employees are bringing into the office (39 percent to 25 percent for larger organizations). Armed with that knowledge, SMOs are more likely to look for malicious infections, with 1 in 3 SMOs saying they had checked the Bring Your Own Device (BYOD) devices in the last month. While just 1 in 5 larger enterprises said they had run the same checks. That despite the higher rate of BYOD polices at larger organizations (see more on that at right).

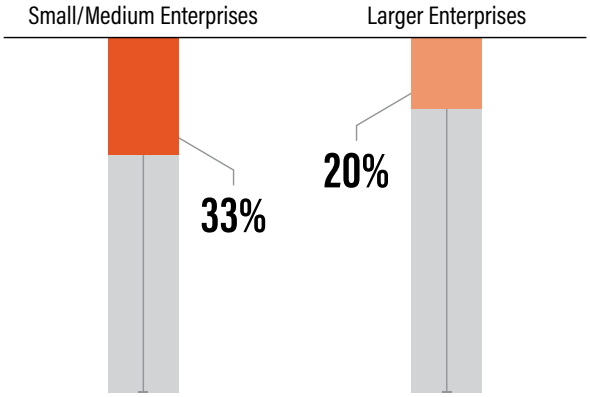
GRAPH 04 **DO YOU KNOW HOW MANY CONNECTED DEVICES YOUR EMPLOYEES ARE BRINGING INTO WORK?**

YES



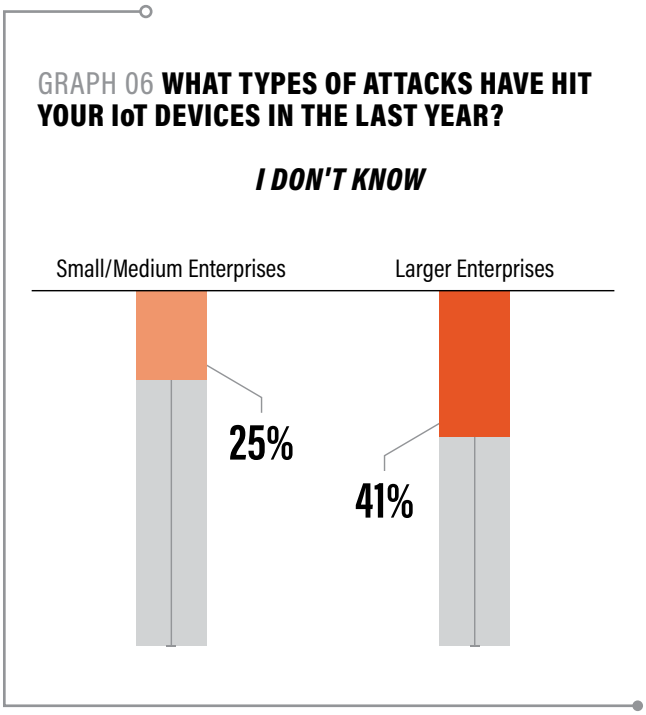
GRAPH 05 **WHEN WAS THE LAST TIME YOU CHECKED DEVICES EMPLOYEES BRING INTO YOUR OFFICE FOR MALICIOUS INFECTIONS?**

IN THE LAST MONTH



→ 41 percent of the large organizations told us they didn't know what types of attacks have hit their IoT devices in the last year. Meanwhile, 25 percent of SMOs said they didn't know what attacks struck their offices.

GRAPH 06 **WHAT TYPES OF ATTACKS HAVE HIT YOUR IoT DEVICES IN THE LAST YEAR?**

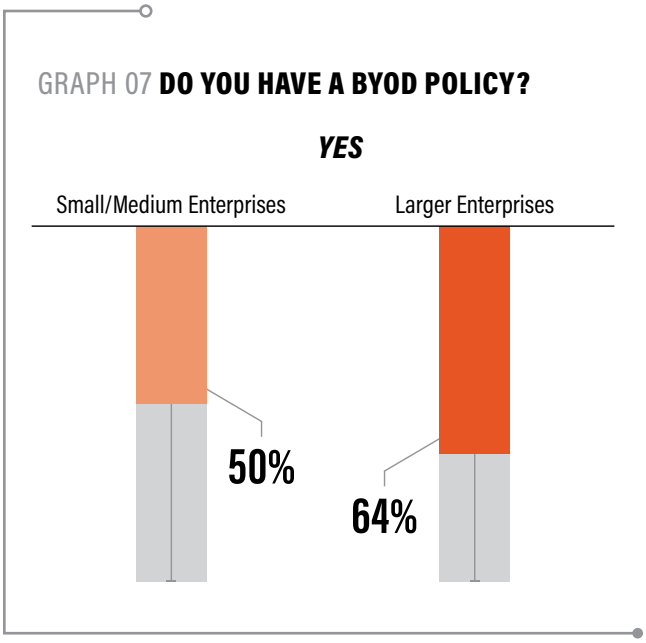


That said, SMOs still face enormous challenges. Much like the organizations in Europe and Asia hard hit by WannaCry, small and midsized organizations are much more likely to be working off older devices and less likely to have IT teams installing the patches needed to keep older software up to date.

LARGE ORGANIZATIONS ARE MORE LIKELY TO TALK A GOOD GAME

One encouraging number from the 340 "large" organizations: IT security professionals working there said their employers were 14 percent more likely to have a BYOD policy than SMOs (64 percent to 50 percent).

GRAPH 07 **DO YOU HAVE A BYOD POLICY?**

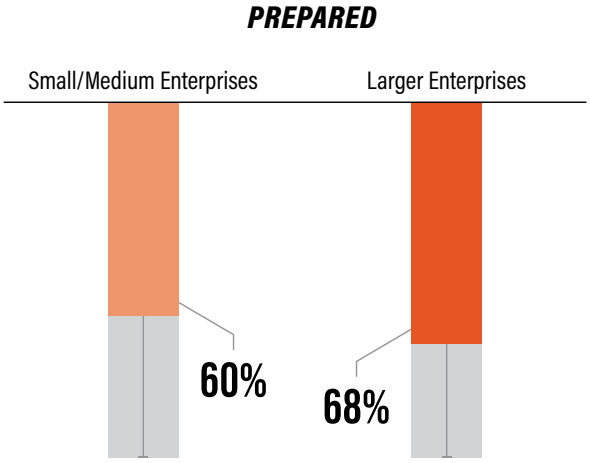


Despite all the data that shows SMOs are better prepared to deal with IoT threats, larger businesses were more likely to say they were prepared. In other words, IT pros at large businesses say they are prepared, but the IT pros at SMOs take more action.

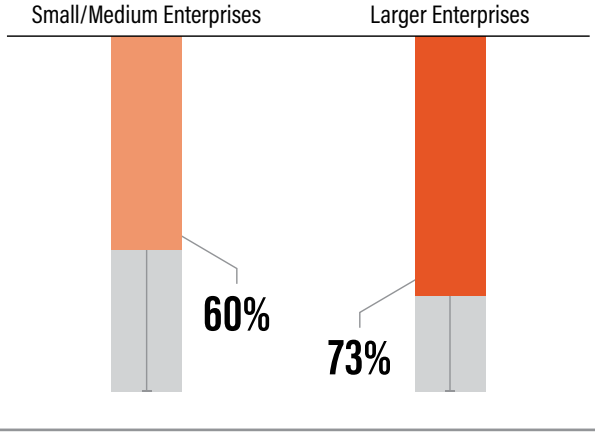
Despite all the numbers that show SMOs are running checks and keeping up with what devices are in their workspace, large organizations are 8 percent more likely to say they are prepared to detect connect device threats.

That gap grows when organizations are asked about their ability to respond to threats via connected devices with 73 percent of large organizations saying they are prepared compared to 60 percent of small/medium organizations.

GRAPH 08 **HOW PREPARED IS YOUR ORGANIZATION TO DETECT CONNECTED DEVICE THREATS?**



GRAPH 09 **HOW PREPARED IS YOUR ORGANIZATION TO RESPOND TO CONNECTED DEVICE THREATS?**



Beyond knowing what devices are on the network, larger enterprises are not identifying risks or assessing threats against their IoT devices as well as SMOs. It is clear to us that large organizations may have a false sense of confidence in regards to IoT security and connected device threats.

BEHIND THE NUMBERS

Because the findings were different from what we expected, Pwnie Express researchers did a deeper dive into the numbers to see if there might be an explanation for why small organizations did better in IoT security. We did find one possible explanation for the surprising results.

Of 610 small/midsized organizations surveyed, 253 of them (or 41 percent) were technology companies. Of the large organizations, only 22 percent (75 respondents) were technology companies. Who better understands the need for cybersecurity than the organizations operating in the digital world? The lesson that can be taken from these numbers is that some industrial titans could benefit from thinking like a tech startup when it comes to security.

CALL TO ACTION

Make no mistake; larger organizations are still infinitely better situated to address cyber attacks than smaller and midsized operations. However, we do believe that the IT security teams at bigger operations are not adapting to the new threat posed by IoT and connected devices. For that matter, small and midsized organizations should be moving faster too, but the IT security pros working in smaller organizations are taking more steps to identify, assess, and respond to IoT based threats.

It is our hope that the larger organizations see this and recognize the need to:

- Recognize that new IoT based business systems—HVAC, TVs, printers, even some kitchen appliances—introduce risk alongside their business optimization. Buyers need to know what to look for before they bring devices into the building and IT security pros need to know what to look for once new devices are there.
- Include new technology to monitor device threats.
- Be sure the security measures in use can assess threats and offer guidance on what devices need immediate concern.

The lesson learned from Mirai and WannaCry: our devices that we rely on for business and pleasure can be weaponized against us. It is time to step up, be more nimble, and challenge the IT teams that have done so well with security for wired and wireless devices to take on the next challenge: the Internet of Things.

Organizations, of all sizes, integrating IoT to gain a competitive advantage could find the tables turn quickly if they don't take the proper precautions to address the IoT security gap.

ENDNOTES

1 IoT's Challenges and Opportunities in 2017: A Gartner Trend Insight Report, Published: 5 April 2017 ID: G00324746, Analyst(s): Mark Hung

2 http://www.techrepublic.com/article/98-of-wannacry-victims-were-running-windows-7-not-xp/

3 http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

4 Ibid.

5 https://signup.keepersecurity.com/state-of-smb-cybersecurity-report/

6 https://www.carbonite.com/globalassets/files-white-papers/carbonite-ransomware-report.pdf

IDENTIFY, ASSESS, AND RESPOND TO IoT THREATS

Pwnie Express closes the IoT security gap exposed by the deployment of IoT in the enterprise. By continuously identifying and assessing all devices and IoT systems, our IoT security platform prevents IoT based threats from disrupting business operations. All without the need for agents, or changes to network infrastructure.

Our easy to deploy and operate SaaS platform, Pulse, makes it easy for security teams to identify, assess, and respond to IoT based threats to prevent business disruption:

- Identify—Discover, take inventory, and classify all IT and IoT devices and build a comprehensive identity for each device.
- Assess—Device behaviors are analyzed to understand system relationships and then monitored to detect threats and risks to business-critical systems.
- Respond—Ensure the safety and compliance of critical systems by preventing business disruption with directed response and shareable intelligence.

TO LEARN MORE ABOUT PWNIE EXPRESS VISIT **WWW.PWNIEEXPRESS.COM**.

Pwnie Express Pwnie Express @PwnieExpress

268 SUMMER STREET, FLOOR 2 • BOSTON, MA 02210 • T: (855) 793-1337 • F: (857) 263-8188